(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

525229

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
1. April 2004 (01.04.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/027587 A2

(51) Internationale Patentklassifikation[7]: G06F 1/00

(21) Internationales Aktenzeichen: PCT/EP2003/008024

(22) Internationales Anmeldedatum:
23. Juli 2003 (23.07.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 38 093.7 21. August 2002 (21.08.2002) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **AUDI AG** [DE/DE]; 85045 Ingolsdadt (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **FEILEN, Oliver** [DE/DE]; Ottersrieder Strasse 20, 85296 Rohrbach (DE). **STADTMÜLLER, Rüdiger** [DE/DE]; Josef-Fleischmann-Strasse 15A, 85055 Ingolstadt-Etting (DE).

(74) Anwalt: **PATZELT, Heike**; Audi AG, Patentabteilung, Postfach 1144, 74148 Neckarsulm (DE).

(81) Bestimmungsstaat *(national)*: US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

Erklärungen gemäß Regel 4.17:

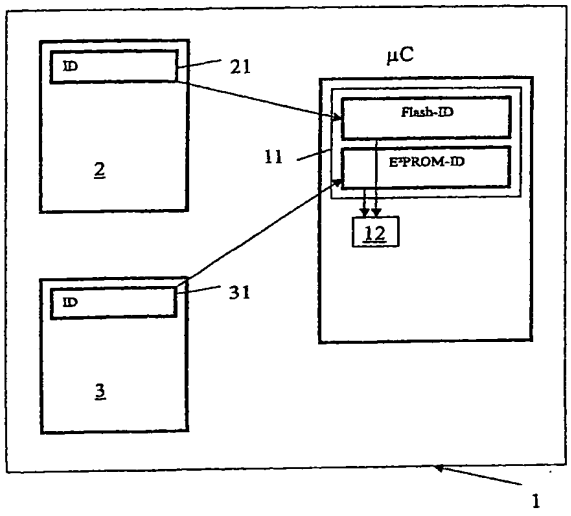
— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR)*

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR)*

[Fortsetzung auf der nächsten Seite]

(54) **Title:** METHOD FOR PROTECTING AT LEAST ONE MOTOR VEHICLE COMPONENT AGAINST MANIPULATION IN A CONTROL DEVICE, AND CONTROL DEVICE

(54) **Bezeichnung:** VERFAHREN ZUM SCHUTZ VOR MANIPULATIONEN AN EINEM STEUERGERÄT FÜR MINDESTENS EINE Kfz-KOMPONENTE UND STEUERGERÄT



(57) **Abstract:** The invention relates to a method for protecting at least one motor vehicle component against manipulations in a control device, comprising at least one micro-computer (µC) and at least one memory component (2, 3). The invention is characterised in that the micro-computer (µC) reads and memorises a specific, original identification (ID) of at least one component (2, 3) of a memory component (2, 3). The invention also relates to a control device for a motor vehicle component, comprising at least one micro-computer (µC) and at least one memory component (2, 3). The invention is characterised in that the at least one memory component (2, 3) comprises at least one specific identification (ID) and the micro-computer (µC) comprises at least one area (11) wherein the at least one specific, original identification is stored.

[Fortsetzung auf der nächsten Seite]

WO 2004/027587 A2

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum Schutz vor Manipulationen an einem Steuergerät für mindestens eine Kfz-Komponente, das zumindest einen Microrechner (µC) and zumindest einen Speicherbaustein (2, 3) umfasst, dadurch gekennzeichnet, dass der Microrechner (µC) eine spezifische, ursprüngliche Kennung (ID) des mindestens einen Speicherbausteins (2, 3) von dem Speicherbaustein (2, 3) ausliest und speichert. Weiterhin bezieht sich die Erfindung auf ein Steuergerät für eine Kfz-Komponente, das zumindest einen Microrechner (µC) und zumindest einen Speicherbaustein (2, 3) umfasst, dadurch gekennzeichnet, dass der mindestens eine Speicherbaustein (2, 3) zumindest eine spezifische Kennung (ID) aufweist and der Mikrocomputer (µC) zumindest einen Bereich (11) aufweist in dem die mindestens eine spezifische, ursprüngliche Kennung abgelegt ist.

Verfahren zum Schutz vor Manipulationen an einem Steuergerät für mindestens eine Kfz-Komponente und Steuergerät

Beschreibung

Die vorliegende Erfindung betrifft ein Verfahren zum Schutz vor Manipulationen an einem Steuergerät für mindestens eine Kfz-Komponente sowie ein Steuergerät.

In Kraftfahrzeugen werden heutzutage zur Steuerung einzelner Kfz-Komponenten Steuergeräte verwendet, wie beispielsweise das Motorsteuergerät oder das Getriebesteuergerät. Die zum Betrieb von solchen Steuergeräten erforderlichen Informationen, wie beispielsweise Programme und Daten, werden verschlüsselt oder unverschlüsselt in Speicherbausteinen (E^2PROM, Flash und dergleichen) abgelegt. Das Verschlüsselungsverfahren ist dabei unabhängig von einer festen Hardware-Kombination von Bausteinen und in der Regel in einem wiederbeschreibbaren Speichermedium abgelegt.

Der Nachteil solcher Steuergeräte und der verwendeten Programme besteht darin, dass einzelne Speicherbausteine ausgetauscht werden können, bzw. die Daten auf den Speicherbausteinen über eine Diagnoseschnittstelle oder über direkten Zugriff auf den Speicherbaustein überschrieben werden können. Der Austausch eines Speicherbausteins oder das Überschreiben der auf diesem Speicherbaustein gespeicherten Daten und Programme kann dazu führen, dass die Kfz-Komponente mit anderen Kenndaten arbeitet. Dies wird beispielsweise bei dem sogenannten Chip-Tuning durchgeführt, bei dem Speicherbausteine, die dem Motorsteuergerät zugeordnet sind, ausgetauscht bzw. die auf diesen Speicherbausteinen gespeicherten Programme und Daten, wie Kenndaten, geändert werden. Dadurch kann beispielsweise eine Erhöhung der Leistung und/oder des Drehmoments des Motors erzielt werden. Wird diese Manipulation durchgeführt ohne die weiteren Kfz-Komponenten, wie Ölkühler, Turbolader oder Bremsen anzupassen, so kann es zu Schäden an diesen Kfz-Komponenten und sicherheitskritischen Zuständen kommen.

Aufgabe der vorliegenden Erfindung ist es daher, ein Steuergerät für Kfz-Komponenten und ein Verfahren zum Schutz vor Manipulationen an einem Steuergerät zu schaffen, bei dem ein Austausch eines Speicherbausteins und die Änderung der Daten sowie Code auf dem Speicherbaustein nicht möglich ist, ohne die Funktionsfähigkeit des Steuergeräts zu beeinflussen oder zumindest die Veränderung zu diagnostizieren und diese ggf. zur Anzeige zu bringen.

Der Erfindung liegt die Erkenntnis zugrunde, dass diese Aufgabe gelöst werden kann, indem eine Kennung der Speicherbausteine eines Steuergeräts, die nicht verändert werden kann, als Identifikationsmittel verwendet wird.

Die Aufgabe wird daher nach einem ersten Aspekt der Erfindung gelöst durch ein Verfahren zum Schutz vor Manipulationen an einem Steuergerät für mindestens eine Kfz-Komponente, das zumindest einen Microrechner (μC) und zumindest einen Speicherbaustein umfasst, wobei der Microrechner eine spezifische, ursprüngliche Kennung des mindestens einen Speicherbausteins von dem Speicherbaustein ausliest und speichert.

Durch Sicherung der urspünglichen Kennung von Speicherbausteinen wird eine Konstante gegeben, die zur Erkennung des Austauschs eines Speicherbausteins oder der Manipulation von Daten dienen kann. Die Kennung kann eine Identifikationsnummer des Speicherbausteins darstellen. Es ist aber auch möglich, als Kennung Daten, die zu einem bestimmten Zeitpunkt aufgenommen wurden, in Form eines Fingerprints zu verwenden. Schließlich kann die Kennung weitere Informationen, wie beispielsweise das Herstellungsdatum bzw. das Datum der ersten Inbetriebnahme des Steuergeräts beinhalten.

Vorzugsweise wird die mindestens eine Kennung in einem nur einmalig beschreibbaren OTP (one-time-programmable)-Bereich des Microrechners abgelegt. Dadurch kann eine Modifikation der Kennung in dem Microrechner verhindert werden und so der Schutz vor Manipulationen erhöht werden.

Die in dem Microrechner gespeicherten Kennungen werden in dem erfindungsgemäßen Verfahren zumindest teilweise zur Authentifizierung von Speicherbausteinen verwendet. Bei jedem Hochfahren des Steuergeräts können anhand der ursprünglichen Kennungen, die in dem Microrechner ab-

gelegt sind, die tatsächlich mit dem Microrechner verbundenen Speicherbausteine einer Authentifizierung unterzogen werden.

In einer Ausführungsform kann die Authentifizierung der Speicherbausteine durch Vergleich der ursprünglichen Kennung mit einer aktuellen Kennung erfolgen. Hierbei werden bei der Inbetriebnahme des Steuergeräts von dem Microrechner die aktuellen Kennungen der mit dem Microrechner verbundenen Speicherbausteine ausgelesen und mit den ursprünglichen Kennungen, die in dem Microrechner abgelegt sind, verglichen. Dadurch kann ein Austausch eines oder mehrerer der Speicherbausteine erkannt und Maßnahmen durchgeführt werden, beispielsweise kann eine Betätigung des Steuergeräts durch den Microrechner verhindert werden.

Alternativ oder zusätzlich kann eine Authentifizierung der Speicherbausteine durch Verschlüsselung von Daten oder Programmen erfolgen, wobei der Schlüssel mindestens einen Teil einer der ursprünglichen Kennungen beinhaltet. Dadurch kann erzielt werden, dass bei Abweichung der Kennung von einer ursprünglichen Kennung der Microrechner nicht auf Daten oder Programme zugreifen kann und das Steuergerät damit nicht lauffähig ist.

Die unverschlüsselt oder verschlüsselt auf zumindest einem der Speicherbausteine abgelegten Daten oder Programme können in Form eines Fingerprints dargestellt werden, der die Daten und Programme zu einem gewissen Zeitpunkt festhält. Werden die Daten oder Programme geändert, so kann bei der erneuten Erfassung des Fingerprints durch Vergleich mit dem verschlüsselt abgelegten Fingerprint eine Manipulation erkannt werden.

Gemäß einem zweiten Aspekt der Erfindung wird die Aufgabe gelöst durch ein Steuergerät für eine Kfz-Komponente, das zumindest einen Microrechner (μC) und zumindest einen Speicherbaustein umfasst, wobei der mindestens eine Speicherbaustein zumindest eine spezifische Kennung aufweist und der Microcomputer zumindest einen Bereich aufweist, in dem die mindestens eine spezifische, ursprüngliche Kennung abgelegt ist.

Um die Manipulation durch Veränderung der in dem Microrechner abgelegten Kennung zu verhindern, kann der Microrechner einen Bereich, der nur einmalig beschreibbar ist (OTP-Bereich), aufweisen und die spezifische, ursprüngliche Kennung des mindestens einen Speicherbausteins in diesem

Bereich abgelegt sein. Dieser OTP-Bereich kann zusätzlich lesegeschützt ausgestaltet sein.

Das Steuergerät kann zusätzlich eine Authentifizierungseinheit zur Authentifizierung der mit dem Microrechner verbundenen Speicherbausteine aufweisen, wobei diese ein Programm, das auf dem Microrechner abgelegt ist, darstellen kann.

Die Authentifizierungseinheit kann daher durch ein Programm gebildet werden, das auf dem Microrechner abgelegt ist und dem Vergleich der ursprünglichen Kennungen mit zumindest einer aktuellen Kennung zumindest eines Speicherbausteins dient. Alternativ oder zusätzlich kann das Programm zur Verschlüsselung von Daten oder Programmen auf mindestens eine der in dem Microrechner gespeicherten ursprünglichen Kennungen zugreifen.

Mindestens einer der Speicherbausteine des Steuergeräts kann in dem Microrechner integriert sein. Es kann sich dabei um einen embedded Flash-Speicher oder um eine E²PROM Emulation im embedded Flash Speicher handeln. . Auch in diesem Fall kann das Ablegen einer Kennung des Speicherbausteins in einem OTP-Bereich des Microrechners vorteilhaft genutzt werden. Analog zu externen Speichern kann eine Authentifizierung der Speicherbausteine durch Verschlüsselung von Daten oder Programmen erfolgen, wobei der Schlüssel mindestens einen Teil einer der ursprünglichen Kennungen beinhaltet. Dadurch kann erzielt werden, dass bei Abweichung der Kennung von einer ursprünglichen Kennung der Microrechner nicht auf Daten oder Programme zugreifen kann und das Steuergerät damit nicht lauffähig ist.

Merkmale und Details, die im Zusammenhang mit dem erfindungsgemäßen Verfahren beschrieben werden, gelten entsprechend für das erfindungsgemäße Steuergerät und umgekehrt.

Die Erfindung wird im Folgenden anhand der beiliegenden Zeichnungen, die sich auf mögliche Ausführungsbeispiele der Erfindung beziehen, beschrieben. Es zeigen:

~~Figur 1: eine schematische Blockdarstellung einer ersten Ausführungsform~~ des erfindungsgemäßen Steuergeräts;

Figur 2: ein Flussdiagramm, das eine Ausführungsform des erfindungsgemäßen Verfahrens darstellt;

Figur 3: eine schematische Blockdarstellung einer zweiten Ausführungsform des erfindungsgemäßen Steuergeräts; und

Figur 4: eine schematische Blockdarstellung einer dritten Ausführungsform des erfindungsgemäßen Steuergeräts.

In Figur 1 ist eine Ausführungsform eines erfindungsgemäßen Steuergeräts dargestellt. Der Aufbau von Steuergeräten, wie beispielsweise Motorsteuergeräten, ist hinlänglich aus dem Stand der Technik bekannt, so dass hierauf nur insoweit eingegangen wird, wie dies für das Verständnis der Erfindung erforderlich ist. Das Steuergerät 1 umfasst in der dargestellten Ausführungsform einen Microcomputer μC, einen Flash-Speicher 2 und einen EEPROM (E^2PROM) 3. Der Flash-Speicher 2 und der E^2PROM 3 weisen jeweils einen OTP-Bereich 21, 31 auf. Diese sind vorzugsweise nicht lesegeschützt ausgestaltet. Auch in dem μC ist ein OTP-Bereich 11 vorgesehen. Weiterhin ist in dem μC eine Authentifikationseinheit 12 enthalten. Diese kann eine elektronische Schaltung oder ein Programm in dem μC darstellen.

Die Speicherbausteine Flash 2, E^2PROM 3 sind in der dargestellten Ausführungsform mit bausteinindividuellen Identifikationsnummern ID versehen. Diese werden in der Regel beim Hersteller des Bausteins geschrieben und in den OTP-Bereich 21, 31 der einzelnen Bausteine abgelegt.

In Figur 2 ist ein Flussdiagramm gezeigt, das eine Ausführungsform des erfindungsgemäßen Verfahrens anhand der in Figur 1 gezeigten Ausführungsform des Steuergeräts darstellt.

Im Herstellungsprozess des Steuergeräts werden erfindungsgemäß bei der Erstinbetriebnahme des Steuergeräts von dem Microrechner μC die ID's der einzelnen Speicherbausteine 2, 3 ausgelesen und in einen einmalig beschreibbaren OTP-Bereich 11 des μC abgelegt. Ab diesem Zeitpunkt ist die Funktion des Steuergeräts 1 nur in Verbindung mit den dem μC bekannten ID's der externen Speicherbausteine 2, 3 möglich.

Bei jeder weiteren Inbetriebnahme des Steuergeräts 1 wird von dem μC die ID aller mit diesem verbundenen Speicherbausteine 2, 3 erneut ausgelesen. In einer Vergleichseinheit können dann diese aktuellen ID's mit den ursprünglichen Kennungen, die in dem OTP-Bereich 11 des μC abgelegt sind, verglichen werden. Wird bei diesem Vergleich festgestellt, dass eine der ID's nicht mit einer der ursprünglichen ID's übereinstimmt, so wird das Steuergerät an seiner Funktion gehindert oder zumindest die Veränderung diagnostiziert und diese ggf. zur Anzeige gebracht

In Figur 3 ist eine weitere Ausführungsform des erfindungsgemäßen Steuergeräts 1 gezeigt. Der Aufbau ist im wesentlichen gleich dem Aufbau der Ausführungsform aus Figur 1, allerdings ist in dieser Ausführungsform der Code zum Betreiben des Steuergeräts in einen Master-Code (MC) und einen Sub-Code (SC) unterteilt. Der Mastercode MC enthält elementare, essentielle Funktionalitäten zum Betrieb des Steuergeräts, z.B. das Programm zur Signalerzeugung für angeschlossene Aktuatoren (nicht dargestellt) des Steuergeräts oder das Programm für die Berechnung der Stellgrößen und Stellwerte. Der Mastercode MC kann weiterhin Daten umfassen. In dem Sub-Code SC sind weitere Programme und Daten enthalten. Das Steuergerät ist nur funktionsfähig unter Verwendung beider Codes MC und SC. In der dargestellten Ausführungsform ist der Sub-Code SC in einem wiederbeschreibbaren Bereich des Flash-Speichers 2 enthalten. Der Master-Code MC ist in einem OTP-Bereich 11 des Microrechners μC enthalten. Der Master-Code ist vorzugsweise gegen Auslesen über die Kontaktierung geschützt. Dies kann beispielsweise physikalisch durch Durchlegieren einer Transistorstrecke oder schaltungstechnisch erzielt werden. Der Sub-Code SC kann im Gegesatz zu dem Master-Code MC modifiziert beziehungsweise überschrieben werden. Dies erlaubt ein Updaten des Subcodes oder ein Reprogrammieren.

Der μC weist weiterhin eine Identifikationsnummer μC-ID auf. Auch diese ist in einem lesegeschützten OTP-Bereich des μC abgelegt. In dem E^2PROM sind weitere Daten für den Betrieb des Steuergeräts in einem wiederbeschreibbaren Bereich abgelegt. Diese Daten können beispielsweise Adaptionswerte sowie Leerlaufdrehzahlen bei einem Motorsteuergerät, sein.

Beim Initialisieren des Steuergeräts lernt der Microrechner μC die in dem OTP-Bereich 21, 31 der Speicherbausteine 2, 3 abgelegten und dadurch nicht veränderbaren Identifikationsnummern an und legt diese in einem OTP-

Bereich des Microrechners μC, der optional auch lesegeschützt ausgestaltet sein kann, ab.

Von diesem Zeitpunkt an sind dem Microrechner μC die mit diesem verbundenen Speicherbausteine 2, 3 über ihre ID bekannt.

Zusätzlich können die in dem Microrechner abgelegten ID's der Speicherbausteine auch zur Verschlüsselung von Daten oder Programmen dienen. So können die auf dem E²PROM abgelegten Daten beispielsweise durch ein symmetrisches Verschlüsselungsverfahren codiert werden, in dem der Schlüssel zumindest einen Teil der ID zumindest eines der Speicherbausteine 2, 3 umfasst. Bei einem Motorsteuergerät können in dem E²PROM beispielsweise Lernwerte, Fertigungsdaten, Anpassungswerte und dergleichen gespeichert sein. Zur Verschlüsselung sind grundsätzlich alle symmetrischen Verschlüsselungsverfahren geeignet, die die Einbeziehung eines steuergeräteindividuellen Kennzeichnens erlauben. Vorzugsweise werden die Daten des E²PROM durch einen Schlüssel verschlüsselt, der zusätzlich oder alternativ zu der ID der externen Speicherbausteine die ID des Microrechners μC umfasst. Hierdurch wird eine steuergeräteindividuelle Verschlüsselung erzielt, die ein Austauschen des E²PROMs oder ein Überschreiben der darauf gespeicherten Daten unmöglich macht bzw. den Betrieb des Steuergeräts nach einer solchen Manipulation verhindert. Der Schlüssel wird vorzugsweise in dem RAM-Speicher des Microrechners μC abgelegt. Dadurch wird der Schlüssel bei jedem Hochlaufen des Steuergeräts unter Einbeziehung eines steuergeräteindividuellen Kennzeichens (z.B. der ID des μC und gegebenenfalls der ID's der Speicherbausteine) gebildet und ist somit steuergeräteindividuell.

Weiterhin kann der Subcode SC auf dem Flash-Speicher 2 ganz oder teilweise verschlüsselt abgelegt sein. Auch für diese Verschlüsselung kann die ID der einzelnen Speicherbausteine oder des Microrechners bzw. ein Teil dieser ID in den Schlüssel integriert werden. Die Entschlüsselung der Daten in dem Sub-Code wird durch den Master-Code durchgeführt. Da dieser in einem lesegeschützten Bereich des Microrechners abgelegt ist, kann ein Auslesen des Programms und damit eine Vervielfältigung der Software verhindert werden.

Die Überwachung des Sub-Codes gegenüber Manipulation, die durch den μC im Master-Code sicher gestellt wird, kann auch über andere Verfahren

als der Verschlüsselung erfolgen. So können zusätzlich oder alternativ lineare/CRC-Checksummenbildung oder Hash-Wertbildung verwendet werden. Zur Erkennung einer vorgenommenen Manipulation der Daten und gegebenenfalls Teile des Subcodes werden z.B. über ausgewählte Bereiche lineare Checksummen gebildet und das Ergebnis verschlüsselt als Fingerprint in den Sub-Code eingebracht. Der Mastercode berechnet im Steuergerätebetrieb, beispielsweise bei einem Signal an Klemme 15, über den gleichen vordefinierten Bereich den Vergleichswert (z.B. lineare Checksumme) und prüft diesen gegen den entschlüsselten, im Sub-Code verschlüsselt abgelegten Referenzwert. Die Art der Manipulationserkennung kann beliebig gewählt werden.

Nach der Erkennung einer Manipulation werden vom Master-Code Maßnahmen eingeleitet, die gegebenenfalls zum Steuergeräteausfall führen.

In Figur 4 ist eine weitere Ausführungsform des erfindungsgemäßen Steuergeräts gezeigt. Bei dieser Ausführungsform sind die Speicherbausteine 2 und 3 in den Microrechner μC integriert. Der μC weist hierbei einen embedded Flash-Speicher auf, wobei der E²PROM emuliert wird. Diese Ausgestaltung des Steuergeräts weist zwar den Vorteil auf, dass ein Austausch der Speicherbausteine zuverlässig verhindert werden kann, allerdings sind die Daten bei der Emulation des E²PROM nur blockweise überschreibbar.

Das Verfahren zum Schutz gegen Manipulation erfolgt bei diesem Steuergerät mit internem Speicher im wesentlichen wie das oben für Steuergeräte mit externen Speichern beschriebene. Auch hierbei können insbesondere die Daten des emulierten E²PROM verschlüsselt abgelegt werden und durch einen Schlüssel, der zumindest eine individuelle Kennung des Steuergeräts, wie die μC-ID und/oder die Flash-ID umfasst, entschlüsselt werden. Ebenso können die in dem Subcode, der in dem Flash-Speicher des μC abgelegt ist, enthaltenen verschlüsselten Daten oder Fingerprints durch den Mastercode entschlüsselt werden. Auch hierbei wird vorzugsweise eine steuergeräteindividuelle Kennung in dem Schlüssel integriert.

Die Erfindung ist nicht auf die dargestellten Ausführungsformen beschränkt. So kann als Kennung der einzelnen Speicherbausteine beispielsweise das Herstellungdatum des Steuergeräts in Betracht kommen. Hierdurch kann eine Manipulation während der Garantiezeit verhindert werden.

Weiterhin ist es beispielsweise auch möglich, den zum Betrieb des Steuergeräts notwendige Code vollständig im lesegeschützten OTP-Bereich des μC abzulegen statt diesen aus einem Master-Code und einem Sub-Code zusammenzusetzen.

Das Steuergerät kann im Sinne dieser Erfindung beispielsweise ein Motorsteuergerät, ein Getriebesteuergerät oder auch ein Kombiinstrument darstellen.

Mit einem erfindungsgemäßen Verfahren und dem erfindungsgemäßen Steuergerät können gegenüber herkömmlichen Steuergeräten eine große Anzahl von Vorteilen erzielt werden.

Mit dem erfindungsgemäßen Steuergerät kann auf zuverlässige Weise ein Austausch einzelner oder mehrerer Bausteine verhindert werden, da durch einen solchen Austausch die Funktion des Steuergeräts verhindert werden kann. Das Auslesen eines für die Funktion der Steuerung zwingend erforderlichen Teils des Programms bzw. der Daten ist nicht möglich, wenn dieser Teil in dem lesegeschützten OTP-Bereich abgelegt ist. Damit kann eine Vervielfältigung der Software verhindert werden. Auch ist der Zugriff auf vertrauliche Daten über die Kontaktierung des Bausteins nicht möglich, wenn diese in dem lesegeschützten OTP-Bereich des μC abgelegt sind. Besonders sicher kann das Steuergerät vor Manipulationen geschützt werden, indem es nur in der Kombination von Master- und Sub-Code lauffähig ist. Eine Veränderung des im reprogrammierbaren, gegebenenfalls externen Speicher, z.B. Flash, abgelegten Sub-Codes führt ohne eine Anpassung des Mastercodes zu einem Steuergeräteausfall. Weiterhin können Daten, die beispielsweise auf einem E^2PROM abgelegt sind, steuergeräteindividuell verschlüsselt werden. Auch die Entschlüsselung solcher Daten kann von einer Kennung des Steuergeräts abhängig gemacht werden. Zusätzliche Sicherheit kann dadurch geschaffen werden, dass die Ver- und Entschlüsselung von dem Verbund der einzelnen Bausteine mit den dem μC bekannten ID's abhängig gemacht wird.

Zusammenfassend kann also festgestellt werden, dass durch das Speichern einer unveränderbaren Kennung der Speicherbausteine eines Steuergeräts die Manipulation von Steuergeräten, wie beispielsweise Chip-Tuning bei Motorsteuergeräten, zuverlässig vermieden werden kann.

Patentansprüche

1. Verfahren zum Schutz vor Manipulationen an einem Steuergerät für mindestens eine Kfz-Komponente, das zumindest einen Microrechner (μC) und zumindest einen Speicherbaustein (2, 3) umfasst, dadurch gekennzeichnet, dass der Microrechner (μC) eine spezifische, ursprüngliche Kennung (ID) des mindestens einen Speicherbausteins (2, 3) von dem Speicherbaustein (2, 3) ausliest und speichert.

2. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass die mindestens eine Kennung (ID) in einem nur einmalig beschreibbaren (OTP)-Bereich (11) des Microrechners (μC) abgelegt wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die in dem Microrechner (μC) gespeicherten Kennungen (ID) zumindest teilweise zur Authentifizierung von Speicherbausteinen (2, 3) verwendet wird.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass die Authentifizierung durch Vergleich der ursprünglichen Kennung mit einer aktuellen Kennung erfolgt.

5. Verfahren nach Anspruch 3 oder 4, dadurch gekennzeichnet, dass die Authentifizierung durch Verschlüsselung von Daten oder Programmen erfolgt, wobei der Schlüssel mindestens einen Teil einer der ursprünglichen Kennungen (ID) beinhaltet.

6. Verfahren nach Anspruch 5 dadurch gekennzeichnet, dass Daten, die auf einem Speicherbaustein (2, 3) abgelegt sind, durch einen Schlüssel, der zumindest eine der ursprünglichen Kennungen (ID) umfasst, verschlüsselt werden und auf dem Speicherbaustein (2, 3) verschlüsselt abgelegt werden.

7. Verfahren nach Anspruch 6 dadurch gekennzeichnet, dass die auf dem Speicherbaustein (2) verschlüsselt abgelegten Daten oder Programme zumindest einen Fingerprint umfassen.

8. Steuergerät für eine Kfz-Komponente das zumindest einen Microrechner (μC) und zumindest einen Speicherbaustein (2, 3) umfasst, dadurch gekennzeichnet, dass der mindestens eine Speicherbaustein (2, 3) zumindest eine spezifische Kennung (ID) aufweist und der Microcomputer (μC) zumindest einen Bereich (11) aufweist in dem die mindestens eine spezifische, ursprüngliche Kennung abgelegt ist.

9. Steuergerät nach Anspruch 8, dadurch gekennzeichnet, dass der Microrechner (μC) einen Bereich (11), der nur einmalig beschreibbar ist, aufweist und die spezifische, ursprüngliche Kennung (ID) des mindestens einen Speicherbausteins (2, 3) in diesem Bereich abgelegt ist.

10. Steuergerät nach einem der Ansprüche 8 oder 9, dadurch gekennzeichnet, dass das Steuergerät (1) eine Authentifizierungseinheit (12) zur Authentifizierung der mit dem Microrechner (μC) verbundenen Speicherbausteine (2, 3) aufweist.

11. Steuergerät nach einem der Ansprüche 10, dadurch gekennzeichnet, dass die Authentifizierungseinheit (12) durch ein Programm gebildet wird, das auf dem Microrechner (μC) abgelegt ist und dem Vergleich der ursprünglichen Kennungen (ID) mit zumindest einer aktuellen Kennung (ID) zumindest eines Speicherbausteins (2, 3) dient.

12. Steuergerät nach einem der Ansprüche 10, dadurch gekennzeichnet, dass die Authentifizierungseinheit (12) durch ein Programm gebildet wird, das auf dem Microrechner (μC) abgelegt ist und der Verschlüsselung von Daten dient, wobei das Programm zur Verschlüsselung von Daten oder Programmen auf mindestens eine der in dem Microrechner (μC) gespeicherten ursprünglichen Kennungen (ID) zugreift.

13. Steuergerät nach einem der Ansprüche 8 bis 12, dadurch gekennzeichnet, dass mindestens einer der Speicherbausteine (2, 3) in dem Microrechner (μC) integriert ist.

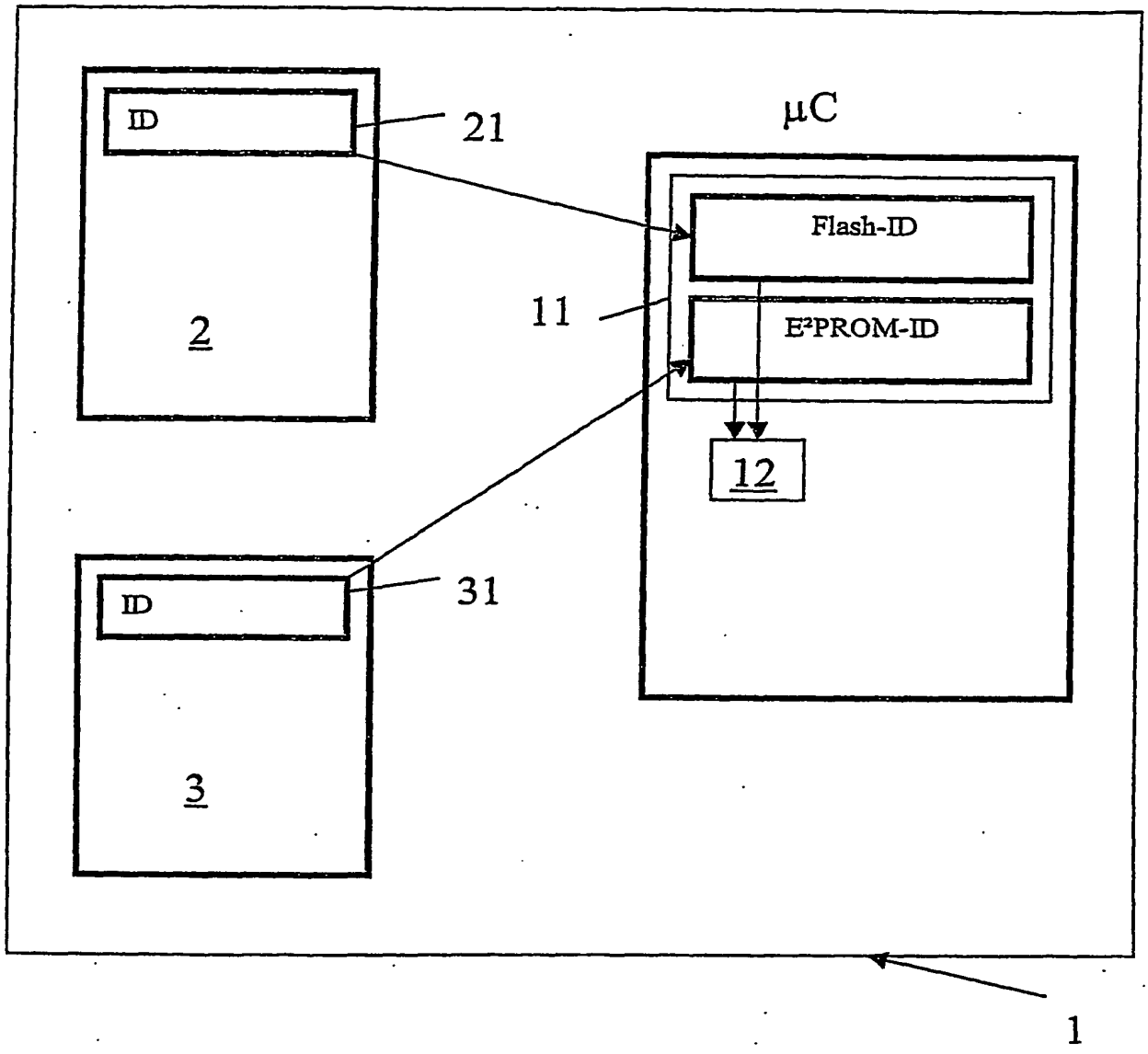


FIG. 1

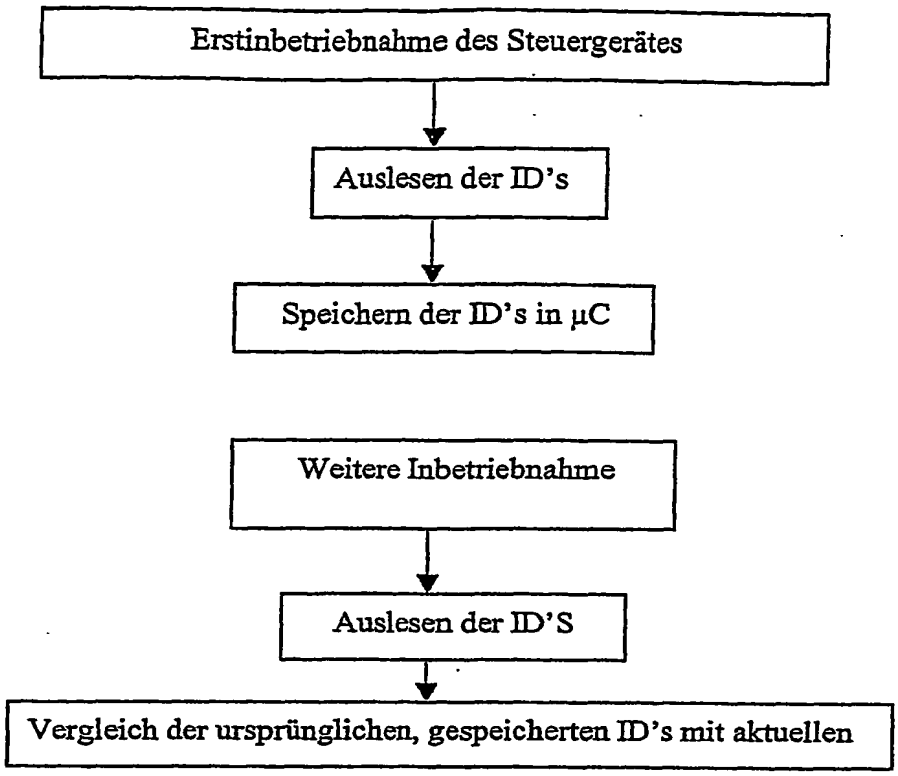

Erstinbetriebnahme des Steuergerätes
Auslesen der ID's
Speichern der ID's in µC
Weitere Inbetriebnahme
Auslesen der ID'S
Vergleich der ursprünglichen, gespeicherten ID's mit aktuellen

FIG. 2

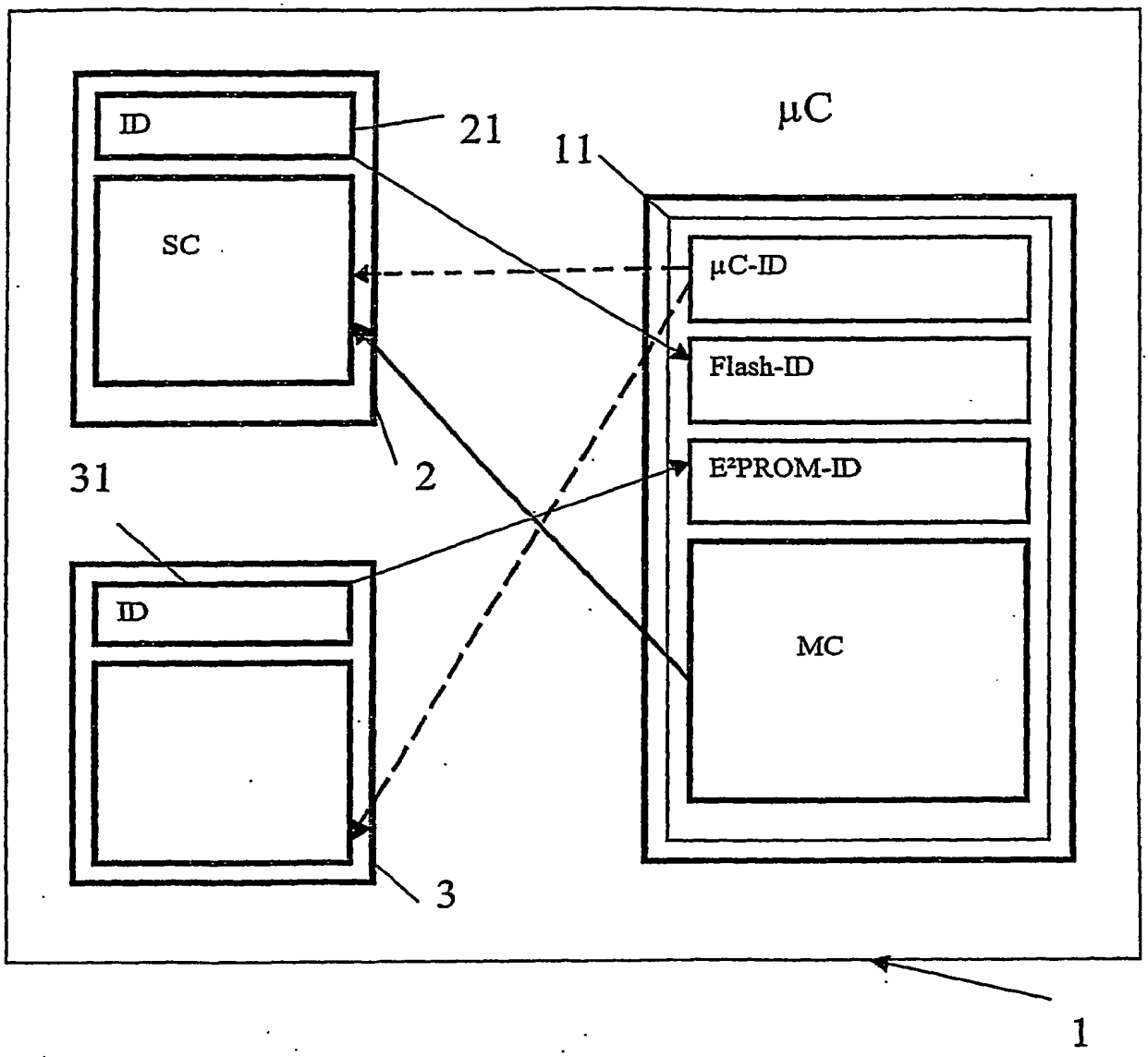


FIG. 3

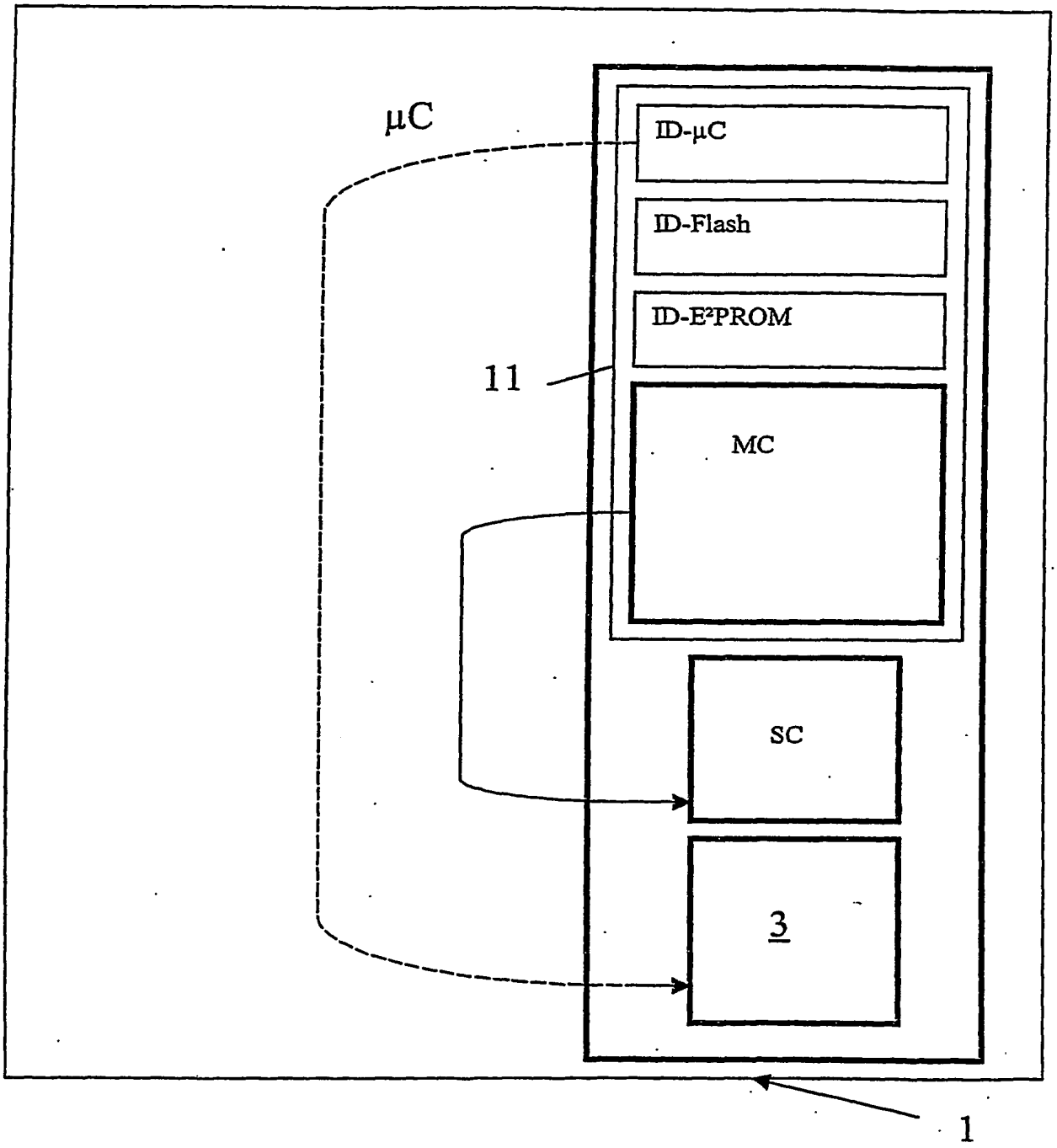


FIG. 4

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
1. April 2004 (01.04.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/027587 A3

(51) Internationale Patentklassifikation[7]: G06F 1/00

(21) Internationales Aktenzeichen: PCT/EP2003/008024

(22) Internationales Anmeldedatum:
23. Juli 2003 (23.07.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 38 093.7 21. August 2002 (21.08.2002) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **AUDI AG** [DE/DE]; 85045 Ingolsdadt (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **FEILEN, Oliver** [DE/DE]; Ottersrieder Strasse 20, 85296 Rohrbach (DE). **STADTMÜLLER, Rüdiger** [DE/DE]; Josef-Fleischmann-Strasse 15A, 85055 Ingolstadt-Etting (DE).

(74) Anwalt: **PATZELT, Heike**; Audi AG, Patentabteilung, Postfach 1144, 74148 Neckarsulm (DE).

(81) Bestimmungsstaat *(national)*: US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

Erklärungen gemäß Regel 4.17:

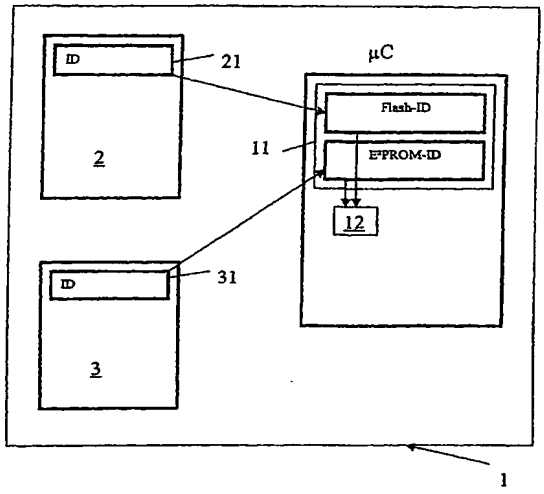
— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR)*

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR)*

[Fortsetzung auf der nächsten Seite]

(54) **Title:** METHOD FOR PROTECTING AT LEAST ONE MOTOR VEHICLE COMPONENT AGAINST MANIPULATION IN A CONTROL DEVICE, AND CONTROL DEVICE

(54) **Bezeichnung:** VERFAHREN ZUM SCHUTZ VOR MANIPULATIONEN AN EINEM STEUERGERÄT FÜR MINDESTENS EINE Kfz-KOMPONENTE UND STEUERGERÄT



(57) **Abstract:** The invention relates to a method for protecting at least one motor vehicle component against manipulations in a control device, comprising at least one micro-computer (µC) and at least one memory component (2, 3). The invention is characterised in that the micro-computer (µC) reads and memorises a specific, original identification (ID) of at least one component (2, 3) of a memory component (2, 3). The invention also relates to a control device for a motor vehicle component, comprising at least one micro-computer (µC) and at least one memory component (2, 3). The invention is characterised in that the at least one memory component (2, 3) comprises at least one specific identification (ID) and the micro-computer (µC) comprises at least one area (11) wherein the at least one specific, original identification is stored.

[Fortsetzung auf der nächsten Seite]

WO 2004/027587 A3

Veröffentlicht:
— *mit internationalem Recherchenbericht*
— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 29. April 2004

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum Schutz vor Manipulationen an einem Steuergerät für mindestens eine Kfz-Komponente, das zumindest einen Microrechner (µC) and zumindest einen Speicherbaustein (2, 3) umfasst, dadurch gekennzeichnet, dass der Microrechner (µC) eine spezifische, ursprüngliche Kennung (ID) des mindestens einen Speicherbausteins (2, 3) von dem Speicherbaustein (2, 3) ausliest und speichert. Weiterhin bezieht sich die Erfindung auf ein Steuergerät für eine Kfz-Komponente, das zumindest einen Microrechner (µC) und zumindest einen Speicherbaustein (2, 3) umfasst, dadurch gekennzeichnet, dass der mindestens eine Speicherbaustein (2, 3) zumindest eine spezifische Kennung (ID) aufweist and der Mikrocomputer (µC) zumindest einen Bereich (11) aufweist in dem die mindestens eine spezifische, ursprüngliche Kennung abgelegt ist.

INTERNATIONAL SEARCH REPORT

[redacted] Application No
PCT/EP 03/08024

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 197 826 A (TOKYO SHIBAURA ELECTRIC CO) 17 April 2002 (2002-04-17) column 1, line 18 - line 22 column 3, line 40 - line 46 column 4, line 26 -column 5, line 22 column 7, line 24 -column 8, line 14	1-13
A	WO 98 58305 A (MCCOLL CAMERON; MEMORY CORP PLC (GB); DEAS ALEXANDER ROGER (GB)) 23 December 1998 (1998-12-23) the whole document	1-13

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 March 2004	19/03/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Sigolo, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/08024

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1197826 A	17-04-2002	WO 0223349 A1	21-03-2002
		US 6490667 B1	03-12-2002
		EP 1197826 A1	17-04-2002
		DE 60007132 D1	22-01-2004
WO 9858305 A	23-12-1998	AU 8028798 A	04-01-1999
		WO 9858305 A1	23-12-1998

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 03/08024

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 1 197 826 A (TOKYO SHIBAURA ELECTRIC CO) 17. April 2002 (2002-04-17) Spalte 1, Zeile 18 - Zeile 22 Spalte 3, Zeile 40 - Zeile 46 Spalte 4, Zeile 26 -Spalte 5, Zeile 22 Spalte 7, Zeile 24 -Spalte 8, Zeile 14	1-13
A	WO 98 58305 A (MCCOLL CAMERON; MEMORY CORP PLC (GB); DEAS ALEXANDER ROGER (GB)) 23. Dezember 1998 (1998-12-23) das ganze Dokument	1-13

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
3. März 2004	19/03/2004

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Sigolo, A

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 03/08024

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 1197826	A	17-04-2002	WO	0223349 A1	21-03-2002
			US	6490667 B1	03-12-2002
			EP	1197826 A1	17-04-2002
			DE	60007132 D1	22-01-2004
WO 9858305	A	23-12-1998	AU	8028798 A	04-01-1999
			WO	9858305 A1	23-12-1998